

Configuração de vários IPs públicos na zona desmilitarizada (DMZ) em roteadores VPN RV042, RV042G e RV082

Objetivo

A Zona Desmilitarizada (DMZ) é uma rede interna de uma organização, que é disponibilizada para uma rede não confiável. De acordo com a segurança, a DMZ fica entre redes confiáveis e não confiáveis. A manutenção da DMZ ajuda a melhorar a segurança da rede interna de uma empresa. Quando uma Lista de Controle de Acesso (ACL) é vinculada a uma interface, suas regras de Elemento de Controle de Acesso (ACE) são aplicadas aos pacotes que chegam a essa interface. Os pacotes que não correspondem a nenhuma das ACEs na Lista de controle de acesso são correspondidos a uma regra padrão cuja ação é descartar pacotes sem correspondência.

O objetivo deste documento é mostrar como configurar a porta DMZ para permitir vários endereços IP públicos e definir a ACL (Access Control List, lista de controle de acesso) para IPs no dispositivo do roteador.

Dispositivos aplicáveis

• RV042

• RV042G

• RV082

Versão de software

• v4.2.2.08

Configuração DMZ

Etapa 1. Faça login na página do Utilitário de configuração da Web e escolha **Setup > Network**. A página *Rede* será aberta:

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

LAN Setting

MAC Address : 50:57:A8:79:F3:7A

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	<input type="button" value="Edit"/>

DMZ Setting

Enable DMZ

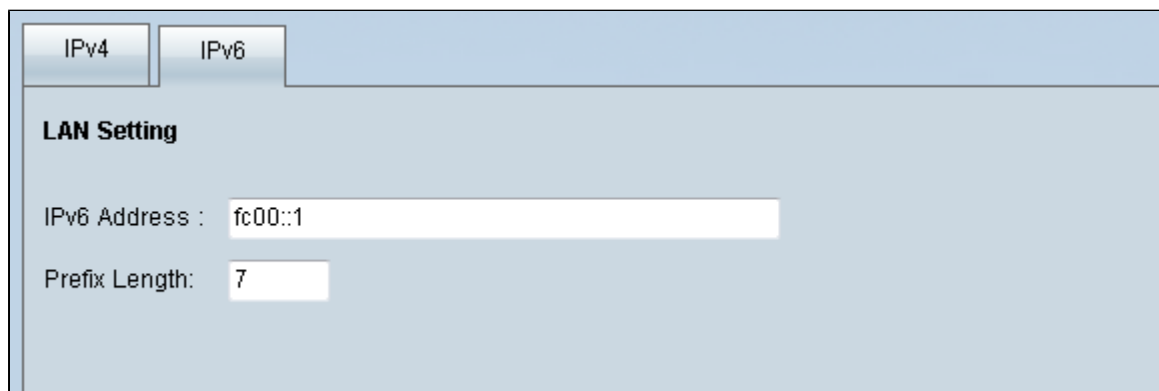
Interface	IP Address	Configuration
DMZ	0.0.0.0	<input type="button" value="Edit"/>

Etapa 2. No *campo IP Mode (Modo IP)*, clique no botão de opção **Dual-Stack IP** para habilitar a configuração de endereços IPv6.

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

Etapa 3. Clique na guia IPv6 localizada no campo *Configuração de LAN* para poder configurar o DMZ no endereço IPv6.




The screenshot shows the 'LAN Setting' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6', with 'IPv6' being the active tab. Below the tabs, the 'LAN Setting' section is visible. It contains two input fields: 'IPv6 Address' with the value 'fc00::1' and 'Prefix Length' with the value '7'.

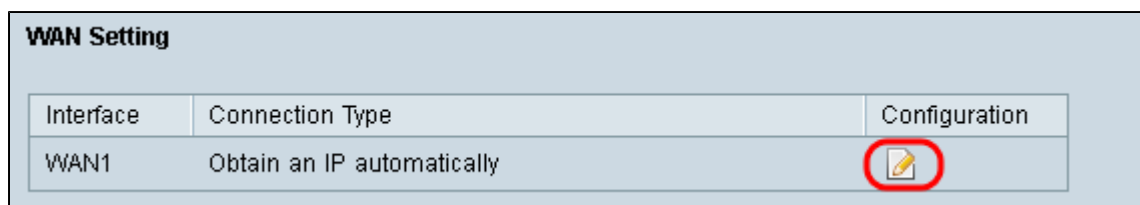
Etapa 4. Role até a área DMZ Setting (Configuração de DMZ) e clique na caixa de seleção **DMZ** para habilitar a DMZ




The screenshot shows the 'DMZ Setting' configuration page. At the top, the 'DMZ Setting' section is visible. It contains a checkbox labeled 'Enable DMZ' which is checked. Below this, there is a table with three columns: 'Interface', 'IP Address', and 'Configuration'. The table has one row with the following data: 'DMZ', '::64', and a pencil icon representing the configuration button.

Interface	IP Address	Configuration
DMZ	::64	

Etapa 5. No campo *Configuração de WAN*, clique no botão **Editar** para editar o IP estático das configurações de WAN1.



The screenshot shows the 'WAN Setting' configuration page. It contains a table with three columns: 'Interface', 'Connection Type', and 'Configuration'. The table has one row with the following data: 'WAN1', 'Obtain an IP automatically', and a pencil icon representing the configuration button. The pencil icon is circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

A página *Rede* é aberta:

The screenshot shows a 'Network' configuration window titled 'Edit WAN Connection'. The interface is set to 'WAN1'. The 'WAN Connection Type' is set to 'Static IP'. The 'Specify WAN IP Address' field contains '192.168.3.1', the 'Subnet Mask' is '255.255.255.0', and the 'Default Gateway Address' is '192.168.3.2'. There are two 'DNS Server (Required)' fields, both containing '0.0.0.0'. The 'MTU' section has 'Auto' selected with a radio button, and 'Manual' is unselected. The 'Manual' option has a text box containing '1500' followed by the word 'bytes'. At the bottom, there are 'Save' and 'Cancel' buttons.

Etapa 6. Escolha **Static IP** na lista suspensa *WAN Connection Type*.

Passo 7. Insira o endereço IP da WAN exibido na página *Resumo do sistema* no campo *Especificar endereço IP da WAN*.

Etapa 8. Insira o endereço da máscara de sub-rede no campo *Subnet Mask*.

Etapa 9. Insira o endereço de gateway padrão no campo *Default Gateway Address*.

Etapa 10. Insira o endereço do servidor DNS que é exibido na página *Resumo do sistema* no campo *Servidor DNS (Obrigatório) 1*.

Observação: o endereço 2 do servidor DNS é opcional.

Etapa 11. Escolha a Maximum Transmission Unit (MTU) para ser **Auto** ou **Manual**. Se você escolher manual, insira os bytes para a MTU Manual.

Etapa 12. Clique na guia **Save** para salvar suas configurações.

Definição de ACL

Etapa 1. Faça login na página do Utilitário de configuração da Web e escolha **Firewall > Access Rules**. A página *Access Rules* será aberta:

Access Rules

IPv4 IPv6

Item 1-3

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always

Add Restore to Default Rules

Observação: Quando você digita a *página Regras de Acesso*, as regras de acesso padrão não podem ser editadas.

Etapa 2. Clique no **botão Adicionar** para adicionar uma nova regra de acesso.

Access Rules

IPv4 IPv6

Item 1-3

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always

Add Restore to Default Rules

A *página Access Rules* agora mostrará opções para as áreas *Service* e *Scheduling*.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Etapa 3. Escolha **Permitir** na lista suspensa *Ação* para permitir o serviço.

Etapa 4. Escolha **All Traffic [TCP&UDP/1~65535]** na lista suspensa *Service* para habilitar todos os serviços para a DMZ.

Etapa 5. Selecione **Registrar pacotes que correspondam a esta regra** na lista suspensa *Registro* para escolher somente os registros que correspondam à regra de acesso.

Etapa 6. Escolha **DMZ** na lista suspensa *Source Interface*. Esta é a origem das regras de acesso.

Passo 7. Escolha **Any** na lista suspensa *Source IP*.

Etapa 8. Escolha **Single** na lista suspensa *Destination IP*.

Etapa 9. Insira os endereços IP do destino para permitir que as regras de acesso no campo *IP de destino*.

Etapa 10. Na área *Agendamento*, escolha **Sempre** na lista suspensa **Tempo** para ativar a regra de acesso o tempo todo.

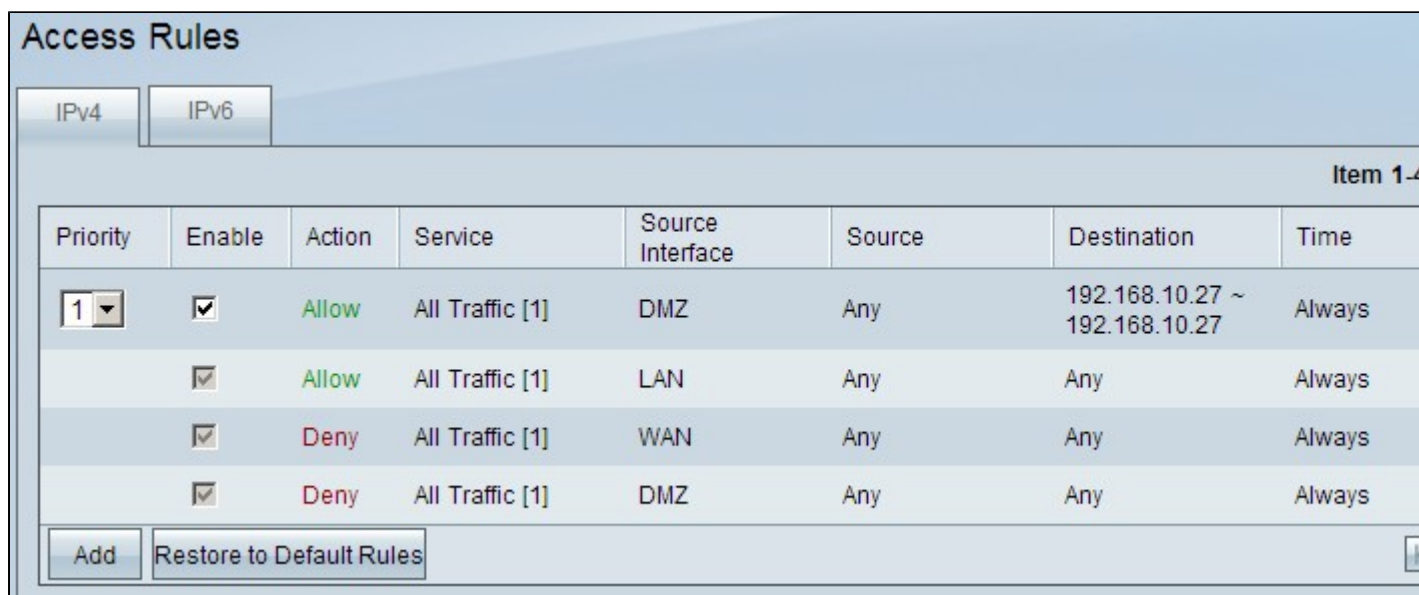
Nota: Se você escolher **Sempre** na lista suspensa **Hora**, a regra de acesso será definida por padrão como **Todos os dias** no campo **Efetivo em**.

Observação: você pode escolher um intervalo de tempo específico (para o qual as regras de acesso estão ativas) selecionando **Intervalo** na lista suspensa **Tempo**. Em seguida, você pode escolher os dias em que deseja que as regras de acesso estejam ativas nas caixas de seleção *Efetivo em*.

Etapa 11. Clique em **Save** para salvar suas configurações.

Nota: Se uma janela pop-up for exibida, pressione 'Ok' para adicionar outra regra de acesso ou pressione 'Cancelar' para retornar à página de Regras de Acesso.

A regra de acesso criada na etapa anterior agora é exibida



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always

Buttons: Add, Restore to Default Rules

Etapa 12. Clique no ícone **Editar** para editar a regra de acesso criada.

Etapa 13. Clique no ícone **Excluir** para excluir a regra de acesso criada.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.